CLAIMS:

1. A method of data hiding comprising the steps of:

providing a message;

providing an encrypting sequence;

generating an encrypted message based on the message and the encrypting sequence;

providing a carrier signal that conveys information unrelated to the encrypted message; and

embedding the encrypted message into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.

2. The method of claim 1, wherein the carrier signal is a digital image.

3. The method of claim 2, wherein the first portion of the carrier signal is an LSB plane of the digital image.

4. The method of claim 1, further comprising the step of embedding the first portion of the carrier signal into a second portion of the carrier signal.

5. The method of claim 4, wherein the carrier signal is a digital image having a plurality of color planes, the first portion of the carrier signal is an LSB plane of a first color plane, and the second portion of the carrier signal is an LSB plane of a second color plane.

6. The method of claim 1, further comprising the steps of transmitting the composite signal to a receiving location, extracting the encrypted message from the composite signal at the receiving location, and decrypting the encrypted message at the receiving location.

7. The method of claim 1, wherein the step of generating an encrypted message includes generating the encrypting sequence based on an encrypting key and performing an exclusive-OR of the message with the encrypting sequence to generate the encrypted message.

8. The method of claim 7, further comprising the steps of transmitting the composite signal to a receiving location, extracting the encrypted message from the composite signal at the receiving location, and decrypting the encrypted message at the receiving location based on the encrypting key.

9. The method of claim 1, wherein the step of providing a message comprised of providing a pre-encrypted message.

10. The method of claim 9, further comprising the step of exchanging an encryption key for decrypting the pre-encrypted message using a trusted third party.

11. A method of data hiding comprising the steps of:

providing an encryption key;

generating an encryption sequence based on the encryption key;

providing a carrier signal that conveys information unrelated to the encryption key; and

embedding the encryption sequence into the carrier signal.

12. The method of claim 11, wherein the encryption key is a public key for an asymmetric encryption algorithm.

13. The method of claim 11, wherein the carrier signal is selected from the group comprising digital images, digital audio, and digital video.

14. The method of claim 11, wherein the encryption sequence is substantially random.

15. The method of claim 14, wherein the encryption sequence is generated based on a linear feedback shift register.

16. The method of claim 11, wherein the step of embedding the encryption sequence includes performing an exclusive-OR of the encryption sequence with a portion of the carrier signal.

17. The method of claim 11, further comprising the steps of transmitting the carrier signal including the embedded encryption sequence to a receiving location, extracting the encryption sequence from the composite signal at the receiving location, and deciphering the encryption sequence to obtain the encryption key at the receiving location.

18. The method of claim 17, further comprising the steps of encrypting a message using the encryption key to generate an encrypted message at the receiving location and transmitting the encrypted message from the receiving location.

19. A method of data hiding comprising the steps of:

embedding an encrypted message into a first portion of a carrier signal; and

embedding message extraction information into a second portion of the carrier signal for extracting the encrypted message from the first portion of the carrier signal.

20. The method of claim 19, wherein the step of embedding an encrypted message includes performing an exclusive-OR of the encrypted message with the first portion of the carrier signal.

21. The method of claim 20, wherein the step of embedding message extraction information includes performing an exclusive-OR of the first portion of the carrier signal with the second portion of the carrier signal.

22. The method of claim 21, wherein the first and second portions of the carrier signal are first and second bit-planes of a digital image.

23. A method of exchanging data hidden in a carrier signal comprising the steps of:

generating a signal including hidden data by transforming a carrier signal from a first domain into a second domain, embedding a message into the carrier signal in the second domain, and transforming the carrier signal back from the second domain to the first domain;

sending the signal including hidden data to a receiving location; and

obtaining the message from the signal including hidden data at the receiving location by transforming the signal including hidden data into the second domain and extracting the message.

24. The method of claim 23, further comprising the steps of encrypting the message prior to generating the signal including hidden data and decrypting the message after obtaining the message from the signal including hidden data.

25. A data hiding apparatus comprising:

an encryption sequence generator configured to generate an encryption sequence based on an encrypting key;

an encrypted message generator configured to generate an encrypted message based on the encryption sequence and an input message; and

an encrypted message embedder configured to embed the encrypted message into a carrier signal.

26. The method of claim 25, wherein the encryption sequence generator is configured to generate a substantially random encryption sequence.

27. The method of claim 25, wherein the encrypted message generator is configured to perform an exclusive-OR of the input message with the encrypting sequence to generate the encrypted message.

28. The method of claim 25, wherein the encrypted message embedder is configured to perform an exclusive-OR of the encrypted message with a portion of the carrier signal.

29. The method of claim 28, wherein the encrypted message embedder is configured to replace a first LSB plane of the digital image with information based on a second LSB plane of the digital image and to perform an exclusive-OR of the encrypted message with the second LSB plane of the digital image.